1969

A Note of a Class of Hadamard Matrices

Jennifer Seberry
University of Wollongong, jennie@uow.edu.au

A Note of a Class of Hadamard Matrices

Abstract

An Hadamard matrix H is a matrix of order n all of whose elements are + 1 or -1 and which satisfies H ffT = nIn . H = S + In is a skew-type Hadamard matrix if ST = -So It is conjectured that an Hadamard matrix always exists for n = 4t, t any integer. Many known matrices and classes of matrices can be found in [1].

Disciplines

Physical Sciences and Mathematics

Publication Details

Jennifer Seberry Wallis, A note on a class of Hadamard matrices, J.Combinatorial Theory, 6, (1969), 222-223.

Reprinted from JOURNAL OF COMBINATORIAL THEORY
All Rights Reserved by Academic Press, New York and London
Vol. 6, No. 2, March 1969
Printed in Belgium

A Note of a Class of Hadamard Matrices

JENNIFER WALLIS

La Trobe University, Bundoora 3083, Victoria, Australia

Communicated by Marshall Hall, Jr.

Received September 9, 1968

An Hadamard matrix H is a matrix of order n all of whose elements are $+1$ or -1 and which satisfies $HH^T = nI_n$. $H = S + I_n$ is a skew-type Hadamard matrix if $S^T = -S$.

It is conjectured that an Hadamard matrix always exists for $n = 4t$, t any integer. Many known matrices and classes of matrices can be found in [1].

In [1, p. 207] it is noted that an Hadamard matrix of order $h(h-1)$ always exists when $h = 2^r(p^s + 1)$, r, s integers and p a prime such that $p^s + 1 \equiv 0 \pmod 4$. We now consider cases $p^s \equiv 1 \pmod 4$.

Let p(prime) $\equiv 1 \pmod 4$ and let $A = (a_{ij})$, $B = (b_{ij})$, $D = (d_{ij})$, all $p \times p$ matrices, be given as follows where $\chi(i)$ is the Legendre symbol modulo p.

$$d_{ij} = \begin{cases} 0 & i = j, \\ \chi(j-i) & i \neq j, \end{cases}$$

$$A = D + I,$$
$$B = D - I.$$

Further define J to be the $p \times p$ matrix of all $+1$'s and $K = J - 2I$ where I is the $p \times p$ unit matrix.

Since J, K, A and B are circulant and symmetric they commute in pairs.

Now
$$JJ^T = pJ_p,$$
$$KK^T = 4I_p + (p-4)J_p,$$
$$DD^T = pI_p - J_p,$$

so
$$AA^T = (D + I_p)(D + I_p)^T = DD^T + 2D + I_p$$
$$= (p+1)I_p - J_p + 2D,$$
$$BB^T = (D - I_p)(D - I_p)^T = DD^T - 2D + I_p$$
$$= (p+1)I_p - J_p - 2D.$$

Then, if

$$M = \begin{bmatrix} J & K \\ -K & J \end{bmatrix} \quad \text{and} \quad N = \begin{bmatrix} A & B \\ B & -A \end{bmatrix},$$

$MM^T = (4I_p + (2p-4)J_p) \times I_2$ and $NN^T = (2(p+1)I_p - 2J_p) \times I_2$.

Since A, B, J, K obey the condition above,

$$MN^T = \begin{bmatrix} JA^T + KB^T & JB^T - KA^T \\ -KA^T + JB^T & -KB^T - JA^T \end{bmatrix}$$

$$= \begin{bmatrix} AJ^T + BK^T & BJ^T - AK^T \\ -AK^T + BJ^T & -BK^T - AJ^T \end{bmatrix} = NM^T.$$

THEOREM 1. *If there exists a skew-type Hadamard matrix $H = S + I_{p-1}$ of order $p-1$, where p(prime) $\equiv 1 \pmod 4$, and if M and N are as defined above then $\overline{H} = S \times N + I_{p-1} \times M$ is an Hadamard matrix of order $2p(p-1)$.*

PROOF:

$$HH^T = (S + I_{p-1})(S^T + I_{p-1}) = SS^T + I_{p-1}$$
$$= (p-1)I_{p-1},$$

so

$$SS^T = (p-2)I_{p-1}.$$

Then

$$\begin{aligned} \overline{H}\overline{H}^T &= (S \times N + I_{p-1} \times M)(S^T \times N^T + I_{p-1} \times M^T) \\ &= SS^T \times NN^T + S \times NM^T + S^T \times MN^T + I_{p-1} \times MM^T \\ &= I_{p-1} \times (4I_p + (2p-4)J_p) \times I_2 \\ &\quad + (p-2)I_{p-1} \times (2(p+1)I_p - 2J_p) \times I_2 \\ &= \{4 + 2(p-2)(p+1)\} I_{2p(p-1)} \\ &= 2p(p-1)I_{2p(p-1)}. \end{aligned}$$

If D is defined by the quadratic residues of $GF(p^r)$, p^r a prime power, instead of by the Legendre symbol we have, similarly,

THEOREM 2. *If there exists a skew-type Hadamard matrix of order $p^r - 1$, where p^r (prime power) $\equiv 1 \pmod 4$, and if M and N are as defined above then $\overline{H} = S \times N + I \times M$ is an Hadamard matrix of order $2p^r(p^r-1)$.*

REFERENCES

1. M. HALL, JR., *Combinatorial Theory*, Blaisdell, Waltham, Mass., 1967.
2. J. WALLIS, A Class of Hadamard Matrices, *J. Combinatorial Theory* **6** (1969), 40–44.

PRINTED IN BRUGES, BELGIUM, BY THE ST. CATHERINE PRESS, LTD.